

MKM:DGR
F.#2017R01838

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

18W 415

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE 6S, MODEL A1688
SEIZED DURING A SEARCH INCIDENT
TO THE ARREST OF DARRELL SPRUILL
ON APRIL 10, 2018, CURRENTLY
LOCATED AT 300 COFFEY STREET,
BROOKLYN, NEW YORK 11231

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Natalie Diaz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”) and NYPD Joint Firearms Task Force (the “Task Force”). In my work with the Task Force, I have participated in numerous investigations of firearms trafficking. I am familiar with the use of cellular phones, computers, and messaging applications to further the sale and trafficking of firearms.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone 6S, Model A1688 seized incident to the arrest of DARRELL SPRUILL on April 30, 2018 (the “Device”). The Device is currently in the custody of the Task Force at 300 Coffey Street, Brooklyn New York 11231.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Since May 2017, the Task Force has been investigating firearms trafficking by DARRELL SPRUILL. During the investigation, the Task Force has used an undercover law enforcement officer (the “UC”) to purchase multiple firearms from SPRUILL, and, for each sale, SPRUILL has communicated with the UC using a cellular phone, first using call number (646) 436-9790 (the “-9790 number”) and then, as of March 2018, using call number (646) 922-2255 (the “-2255 number”).¹

7. On April 26, 2018 a grand jury in the Eastern District of New York returned a sealed indictment charging SPRUILL and others with conspiring to traffick firearms and with trafficking firearms. That day, the Honorable Viktor V. Pohorelsky signed an arrest warrant for SPRUILL’s arrest. On April 30, 2018, SPRUILL was arrested pursuant to that warrant.

¹ On or about March 23, 2018, SPRUILL was arrested by the NYPD. Based on my review of law enforcement databases and communications with the service provider for SPRUILL’s phone, I learned that, following that arrest, SPRUILL changed his assigned call number to (646) 922-2255.

June 2017 Firearm Sale

8. On July 19, 2017, SPRUILL sold multiple firearms to the UC in Brooklyn, New York.

9. Prior to the sale, SPRUILL communicated with the UC via text messages from the -9790 number. SPRUILL sent the UC a picture of a firearm and stated, "this is on its way up". SPRUILL and the UC arranged the sale via text message.

10. On July 19, 2017, the UC drove to the vicinity of Rochester Avenue and Park Place in Brooklyn, New York to meet SPRUILL. Thereafter, SPRUILL arrived and entered the vehicle with the UC. While inside, SPRUILL sold one Jiminez Arms 9mm pistol and ammunition to the UC.

December 2017 and January 2018 Firearms Sales

11. SPRUILL sold multiple firearms to the UC in December 2017 and January 2018.

12. On December 18, 2017, the UC purchased multiple firearms from SPRUILL, which sale was surveilled by the Task Force and consensually recorded by surveillance cameras inside the UC's vehicle. Based on my review of that footage, I am aware that, during the sale, SPRUILL handed the UC multiple firearms and he noted that one firearm was missing its "clip" or magazine. Thereafter, SPRUILL told the UC that he needed to return to "Kingsborough" to get the missing magazine.

13. Thereafter, while in SPRUILL used what I recognize to be an Apple iPhone to make a phone call while inside the UC's vehicle. Based on my review of information from the service provider for the -9790 number, I know that SPRUILL made a call at this approximate time. During that call, SPRUILL is overhead having the following exchange:

SPRUILL: Yo, Bro, um, I don't got the clip for the, um Ruger.

UM: [Inaudible]

SPRUILL: It's in the bag?

UM: [Inaudible]

SPRUILL: Alright, so, um, call your moms. I'm about to come right now.

14. After completing the phone call, SPRUILL exited the vehicle. He returned to the UC's vehicle shortly thereafter, and he handed the UC a magazine for one of the firearms being purchased by the UC.

ONGOING FIREARMS TRAFFICKING

15. After the January 25, 2018 sale by SPRUILL to the UC, SPRUILL contacted the UC using the -9790 number about additional firearms he had for sale.

16. On or about March 6, 2018, the UC contacted SPRUILL via text messages from the -9790 number to inquire about additional firearm purchases. At that time, SPRUILL informed the UC, in sum and substance that his "guy" has not been around and that SPRUILL would inform the UC when he returned. Based on my training and experience, and my conversations with the UC, I understand SPRUILL to have been referring to his firearms supplier.

17. Approximately three weeks later, SPRUILL changed his cellular phone number to (646) 922-2255.

18. SPRUILL text messaged the UC using the new -2255 number, and had the following exchange:

SPRUILL: Yo

UC: Who this

SPRUILL: Milk

UC: Oh. yo whats good yo

* * *

SPRUILL: This my new number my mans got a shotty

Based on my training and experience, my investigation of this case to date, and my debriefing of the UC, I know that "Milk" is a nickname for SPRUILL. Further, I understand that in this exchange, SPRUILL was telling the UC about his new phone number and was telling the UC that he could obtain a shotgun for sale ("my mans got a shotty").

19. Upon his arrest, SPRUILL provide members of the Task Force with the -2255 number as his telephone number during the booking process

20. Accordingly, based on the foregoing there is probable cause to believe SPRUILL has used cellular telephones, including the Device, in furtherance of his trafficking of firearms.

21. The Device is currently in the lawful possession of the Task Force. It came into the Task Force's possession in the following way: On April 30, 2018, members of the Task Force arrested SPRUILL pursuant to an arrest warrant issued by the Honorable Viktor V. Pohorelsky, United States Magistrate Judge, Eastern District of New York. At that time, the Device was in SPRUILL's possession and was seized during the execution of the arrest warrant. Therefore, while the Task Force might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

22. The Device is currently in the custody of the Task Force. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Task Force.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored

images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer

programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

24. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

27. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is

analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

a. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

b. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

c. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.


29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



NATALIE DIAZ
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me
on May 8, 2018



J. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is an Apple iPhone 6S, Model A1688 seized incident to the arrest of DARRELL SPRUILL on April 30, 2018 (the "Device"). The Device is currently in the custody of the Task Force at 300 Coffey Street, Brooklyn New York 11231.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 922, 924, and 371 and involve DARRELL SPRUILL between May 1, 2017 and April 30, 2018, including:

- a. records and information concerning the source of supply for firearms (including names, businesses, addresses, phone numbers, or any other identifying information);
- b. records and information concerning the locations used to store firearms or the proceeds from firearms sales;
- c. information about and lists of firearms customers and related identifying information;
- d. information concerning transactions with firearms customers and related identifying information;
- e. models, calibers, types, and prices of firearms as well as dates and places of any firearms-related transactions;
- f. any information recording SPRUILL's schedule or travel from May 1, 2017 to the present;
- g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address **used** to communicate with firearms purchasers, including the NYPD undercover officer, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.